

Print.App Data Processing Agreement

Parties and background

This Data Processing Agreement (the "DPA") is entered into between:

1. **[Customer legal name]**, [address], [company registration number] (the "Customer" or "Controller"); and
2. **Print.App ApS**, a company registered in Denmark, Njalsgade 21 F, 2. 2300 København S, CVR 45469808 ("Print.App" or "Processor").

The Customer uses Print.App's product personalization software, including the Print.App Editor, under the [Print.App Terms of Service](#) (the "Agreement"). In providing the Agreement, Print.App processes personal data on the Customer's behalf, mainly photographs and other files that the Customer's shoppers ("Users") upload while personalizing products.

The parties sign this DPA so that this processing meets Article 28(3) and (4) of Regulation (EU) 2016/679 (the "GDPR"). Terms such as "personal data", "processing", "controller", "processor", "data subject" and "personal data breach" have the meanings given in the GDPR.

Section I: Purpose, scope and interpretation

1. Purpose and scope. This DPA sets out the obligations of the Controller and the Processor for the processing of personal data described in Annex II ("Customer Personal Data"). Annexes I to IV form part of this DPA.

2. Interpretation. This DPA is read in line with the GDPR. Nothing in it may be read as reducing the protection the GDPR gives to data subjects or as conflicting with the parties' obligations under the GDPR.

3. Hierarchy. If this DPA conflicts with the Agreement or any other arrangement between the parties, this DPA prevails for matters of personal data protection.

4. Scope of roles. For Customer Personal Data, the Customer is the controller and Print.App is the processor. For personal data that Print.App collects to run the Customer's account and billing (name, email, company name and payment details of the Customer's own staff), Print.App is an independent controller under its [Privacy Policy](#), and this DPA does not apply.

Section II: Obligations of the parties

5. Instructions. Print.App processes Customer Personal Data only on the Customer's documented instructions. The Agreement, this DPA and the Customer's configuration of the Print.App service are the Customer's complete instructions; further instructions must be in writing. If Print.App is required by EU or Member State law to process the data otherwise, it will tell the Customer first, unless that law prohibits it. Print.App will tell the Customer promptly if it believes an instruction infringes the GDPR.

6. Purpose limitation. Print.App processes Customer Personal Data only for the purposes in Annex II. It does not use uploaded photographs to train models, to identify the people shown, or for its own marketing.

7. Duration. Processing lasts for the term of the Agreement, then ends as set out in clause 17.

8. Security. Print.App implements at least the technical and organisational measures in Annex III, taking into account the state of the art, the cost of implementation, and the nature, scope, context and purposes of processing. Print.App may update these measures, provided the overall level of security is not reduced.

9. Confidentiality and access. Print.App grants access to Customer Personal Data only to personnel who need it to perform the Agreement, and who are bound by confidentiality obligations.

10. Sensitive data and children. The Customer decides whether its Users may upload photographs showing children or revealing special categories of data, and is responsible for having a lawful basis, including any consent required under Article 8 GDPR. Print.App applies the measures in Annex III to all uploads alike.

11. Documentation and audits.

1. Print.App makes available to the Customer the information needed to show compliance with this DPA and Article 28 GDPR, and answers reasonable questions about its processing.
2. The Customer may audit Print.App's compliance once every 12 months, or after a personal data breach, with at least 30 days' written notice. Audits take place during business hours, at the Customer's cost, and by an auditor bound by confidentiality. Print.App may first offer recent written documentation or third-party certifications instead.
3. Each party makes the information in this clause available to the competent supervisory authority on request.

12. Sub-processors.

1. The Customer gives Print.App general authorisation to engage the sub-processors listed in Annex IV.
2. Print.App will notify the Customer in writing at least 30 days before adding or replacing a sub-processor. The Customer may object on reasonable data protection grounds within that period. If the parties cannot resolve the objection, the Customer may terminate the affected part of the Agreement.
3. Print.App imposes on each sub-processor, by written contract, data protection obligations that are no less protective than this DPA, and remains fully responsible to the Customer for each sub-processor's performance.

13. International transfers.

1. Customer Personal Data is stored in the European Economic Area (EEA), as described in Annex II.
2. Print.App transfers Customer Personal Data outside the EEA only in two cases: temporary caching on Amazon CloudFront edge locations close to the person requesting a file, and, when a User applies a background removal or AI image effect, sending that image to fal.ai in the United States for processing (Annex IV).
3. Transfers to AWS rely on the European Commission's standard contractual clauses in the AWS GDPR Data Processing Addendum and Amazon's EU-U.S. Data Privacy Framework certification. Transfers to fal.ai rely on the European Commission's standard contractual clauses (Implementing Decision (EU) 2021/914) incorporated in fal.ai's Data Processing Addendum.
4. Print.App will not make any other transfer to a third country without the Customer's prior written authorisation and a valid transfer mechanism under Chapter V GDPR.

Assistance and breach notification

14. Assistance to the Controller.

1. Print.App will promptly forward to the Customer any request it receives directly from a data subject, and will not respond itself unless the Customer authorises it.
2. Taking into account the nature of the processing, Print.App assists the Customer with appropriate technical and organisational measures in responding to data subject requests under Chapter III GDPR. In particular, on the Customer's written request, Print.App will permanently delete a data subject's uploaded photographs as described in Annex II, and confirm in writing when done.
3. Print.App assists the Customer with its obligations under Articles 32 to 36 GDPR, including data protection impact assessments and prior consultation, using the information available to Print.App.

15. Personal data breach.

1. Print.App notifies the Customer without undue delay, and in any event within 48 hours, after becoming aware of a personal data breach affecting Customer Personal Data.
2. The notification describes, as far as then known: the nature of the breach, the categories and approximate number of data subjects and records concerned, the likely consequences, the measures taken or proposed, and a contact point. Information not yet available is provided in phases without undue delay.
3. Print.App takes reasonable steps to contain the breach and limit its effects, and helps the Customer notify the supervisory authority and data subjects where Articles 33 and 34 GDPR require it.

Section III: Final provisions

16. Non-compliance and termination. If Print.App breaches this DPA, the Customer may instruct it to suspend the affected processing until it complies. If Print.App does not restore compliance within 30 days, or breaches this DPA seriously or persistently, the Customer may terminate the affected part of the Agreement. Either party may also terminate if a binding decision of a court or supervisory authority on the parties' obligations under the GDPR is not complied with.

17. Deletion and return.

1. When the Agreement ends, the Customer may export its project data and uploaded files within 30 days.
2. After that period, Print.App deletes all Customer Personal Data from its primary storage, unless EU or Member State law requires it to be kept.
3. Copies in backups, caches and temporary processing storage expire on the schedule in Annex II. Until then they stay protected by this DPA and are not used.
4. On request, Print.App confirms the deletion in writing.

18. Liability. Each party's liability under this DPA is subject to the limitations in the Agreement, except where the GDPR does not allow liability towards data subjects to be limited.

19. Governing law. This DPA is governed by the laws of Denmark. The courts of Denmark have exclusive jurisdiction, in line with the Agreement.

Signatures

	Customer (Controller)	Print.App ApS (Processor)
Name		
Title		

	Customer (Controller)	Print.App ApS (Processor)
Date		
Signature		

Annex I: List of parties

	Controller	Processor
Name	[Customer legal name]	Print.App ApS
Address	[Customer address]	Njalsgade 21 F, 2. 2300 København S, Denmark
Registration number	[Customer registration number]	CVR 45469808
Contact for data protection	[name, email]	support@print.app

Annex II: Description of the processing

Data subjects. The Customer's shoppers who use the Print.App Editor (Users), and any people who appear in photographs or text that Users upload or enter.

Categories of personal data.

- Photographs and other image files uploaded by Users. These may show identifiable people, including children.
- Project and design data, including text Users enter (such as names or dates printed on a product) and previews generated from it.
- UserData, where the Customer enables it: a User's name, address, email and phone number, used to fill design fields.
- Order data pushed by webhook, where the Customer enables it: product title and ID, email address, shipping and billing information.

Special categories. Print.App does not request special categories of data. A photograph may incidentally reveal such data; see clause 10.

Nature and purpose. Storing uploads and projects, rendering previews, converting and resizing images, generating print-ready files, and delivering them to the Customer, so Users can personalize products and the Customer can produce orders.

Frequency. Continuous, for the term of the Agreement.

Location. Primary storage in AWS EU-West 1 (Ireland), replicated across three availability zones. Backup copy in AWS EU-North 1 (Stockholm, Sweden). Short-lived processing in AWS regions in France and Germany. Temporary CDN caching as described in clause 13.

Retention.

Data	Where	Kept for
Uploaded photos and project data	Primary storage, Ireland	While the Customer's account is active, or until deleted on request
Backup copy of uploads	Stockholm	Removed within 30 days after deletion from primary storage
Earlier versions of a replaced or deleted file	Ireland and Stockholm	30 days
Database records (projects, UserData, webhook data)	Ireland	While the account is active; point-in-time backups roll off after 35 days
Print files and downloads	Ireland, France	1 to 4 days
Temporary image conversions	Ireland, Germany	14 to 181 days, depending on the process
CDN cached copies	Edge locations	Up to 60 days by default; cleared on a deletion request
Files uploaded with automatic deletion enabled	Ireland and Stockholm	7 days

Annex III: Technical and organisational measures

Area	Measure
Encryption in transit	All traffic to the Editor, API and CDN uses TLS
Encryption at rest	All storage buckets use AES-256 server-side encryption
Storage access	Upload and temporary storage block all public access; files are readable only by Print.App's CDN, which is authenticated to storage by AWS origin access control

Area	Measure
File identifiers	Every upload is stored under a randomly generated identifier, never the original file name
Administrative access	Production access is limited to the account owner, with multi-factor authentication, and one programmatic key for deployment
Service access	Processing functions reach storage through AWS IAM roles, not public links
Availability	Primary data is replicated across three isolated availability zones in Ireland, with a backup copy in Stockholm and 35-day point-in-time recovery for databases
Data minimisation	Temporary files expire automatically under storage lifecycle rules (Annex II)
Deletion	Deletions propagate to the backup copy; earlier file versions expire after 30 days; CDN copies are cleared on deletion requests
Personnel	Customer content is accessed only when needed for support or to run the service
Incident response	Breaches are handled and notified under clause 15

Annex IV: List of sub-processors

Sub-processor	Service	Data processed	Location	Transfer safeguard
Amazon Web Services EMEA SARL	Hosting, storage, databases, CDN	All Customer Personal Data	Ireland, Sweden, France, Germany; CDN edge caching worldwide	AWS GDPR DPA with standard contractual clauses; EU-U.S. Data Privacy Framework

Sub-processor	Service	Data processed	Location	Transfer safeguard
Features & Labels, Inc. (fal.ai)	Background removal and AI image effects, only when a User applies one	The image being processed	United States	fal.ai Data Processing Addendum with standard contractual clauses

Print.App's payment processor, Stripe, handles the Customer's own billing data, for which Print.App is controller. Stripe does not receive Customer Personal Data and is not a sub-processor under this DPA.